CONTINUATION OF APPLICATION FOR A SEARCH WARRANT AND IN SUPPORT OF A CRIMINAL COMPLAINT

INTRODUCTION

1. I, Aaron Eastham, am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed since 2018. I am currently assigned to the Detroit Field Office, Grand Rapids Resident Agency. During my employment with the FBI, I have conducted investigations involving violations of federal criminal laws, including violations related to child exploitation and pornography. I am familiar with the various statutes of Title 18, United States Code, Chapter 110 – sexual exploitation and other abuse of children, including violations pertaining to sexual exploitation and attempted sexual exploitation of children (18 U.S.C. § 2251(a)), distribution or receipt of child pornography (18 U.S.C.§ 2252A(a)(2)) and possession of child pornography (18 U.S.C. § 2252A(a)(5)(B)), the "subject offenses." I am a federal law enforcement officer and, therefore, authorized by the Attorney General to request a Search Warrant under Federal Rule of Criminal Procedure 41.

2. This continuation is made in support of an Application for a Search Warrant for the residence of **3102 Do-Mar Ave, Marne, MI** (hereinafter the "SUBJECT PREMISES"), to search for evidence of coercion and enticement of a minor (contrary to 18 U.S.C. § 2422(b)), as well as for evidence of sexual exploitation of a child (also referred to as production of child pornography, contrary to 18 U.S.C. § 2251), distribution and receipt of child pornography (contrary to 18 U.S.C. § 2252A), and possession of child pornography (contrary to 18 U.S.C. § 2252A). Child pornography is any visual depiction

of a minor depicting the lascivious exhibition of the genitals or sexually explicit conduct, *see* 18 U.S.C. § 2256(8).

3. I also make this Continuation in support of an Application for a Search Warrant for the residence of **Black Samsung cellular phone, IMEI 355802950227157,** (hereinafter the "SUBJECT DEVICE"), to search for evidence of the same offenses listed above.

4. The statements contained in this Continuation are based upon information acquired during my investigation, as well as information provided by others such as other police officers, and task force officers (TFOs) and special agents of the FBI. Because this Continuation is being submitted for the limited purposes described above, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe necessary to establish probable cause to believe that there is evidence of criminal activity in violation of 18 U.S.C. §§ 2251(a), 2252A(a)(2), and 2252A(a)(5)(B) at the SUBJECT PREMISES (further described in Attachment A).

PROBABLE CAUSE FOR SEARCH WARRANT

5. During an Ottawa County Sheriff's Office investigation into an alleged sexual assault of a 16-year-old female by TIMOTHY BAKER ("SUBJECT"), that took place on or around December 4, 2022, a search warrant was executed on BAKER's Snapchat account (username Timothylb81), which he used to communicate with the 16-year-old female.

6. The search warrant return for BAKER's snapchat account revealed the e-

mail bakerjaws1981@gmail.com and phone number 231-903-9494 were associated with the account. The phone number 231-903-9494 was later used by Law Enforcement to make contact with BAKER and set up an interview.

7. A photo was found in the Snapchat records, sent from Snapchat user "poisonivy5995" of a what appeared to be a minor female, sitting on a bed, shirtless, with her breasts exposed. The photo appeared as if the female did not know the photo was being taken. The data contained within the sent picture indicates that it was sent on or around 1/21/2023 at 3:46:16 UTC.

8. A search warrant for the Snapchat account of poisonivy5955 was executed by the Ottawa County Sheriff's Office on March 6, 2023. The Snapchat return provided the account owner's name as SHAELYN FANN and an associated phone number of 231-760-3791. By reviewing local databases, the account owner was identified as:

a. Shaelyn Fann

b. DOB: 6/26/1991

c. Address: 1523 Oregon Avenue in Norton Shores

9. 1523 Oregon Avenue, Norton Shores, Michigan is located in Muskegon County, Michigan.

10. On April 13, 2023, Law Enforcement interviewed FANN. FANN confirmed her phone number was 231-760-3791, which matched the records from the Snapchat account of poisonivy5955. FANN had a daughter who was then 12 years old [MINOR VICTIM 1 (MV1)]. FANN stated that she only talked to her friend TIM BAKER on

Snapchat. FANN confessed to sending BAKER completely nude images of MV1 to BAKER that included pictures of her vaginal area. FANN didn't think that MV knew the pictures were being taken. FANN estimated she sent BAKER 10 to 15 nude or partially nude images of MV1. She sent the images through Snapchat. The sharing of nude photos of MV1 started at the end of the summer of 2022 and stopped a couple of months prior to FANN's interview with law enforcement. During that time, BAKER would regularly send messages, via text and Snapchat, about wanting to have sexual contact with MV1. FANN claimed she took the photos of MV with her phone.

11. FANN consented to allow Law Enforcement to search her phone and the Ottawa County Sheriff's Office took possession of FANN's phone on that date. Later, FANN's consent was revoked.

12. On 6/09/2023, a search warrant was authorized by the 60th District Court for the search of the phone. The phone was then extracted pursuant to the warrant and reviewed. During the review of the phone, text messages were found between FANN and a contact named "Jack." The phone number for "Jack" was 231-903-9494, which was the number used to previously call BAKER and associated with BAKER's Snapchat account. Additionally, the phone number 231-903-9494 sent FANN multiple selfie-style photos in which BAKER's face was plainly visible.

13. In a text message conversation that occurred on or about June 27, 2022, FANN told BAKER that MV1 was 11-years-old. BAKER asked FANN multiple times for pictures of MV1. BAKER told FANN to send the images over Snapchat. Several times

FANN told BAKER she sent a picture of MV1 on Snapchat and BAKER confirmed he received them. BAKER talked about being exited to see MV1's "kitty" and told FANN that it's up to her to make it happen. FANN described a time that she attempted to take a picture of MV1's "kitty" while she was sleeping, but she kept waking up. On one occasion, FANN told BAKER that she "got one" and told BAKER to check Snapchat. BAKER asked if it was a "naked kitty pic" and then said that "It's not terrible can't tell what it is if you hadn't told me" and asked her to resend it to him. FANN then said "She was laying on her side so that's what I could get of between her legs." A few days later the following conversation was had:

Fann: What pics u want?

Baker: The naughtiest the better

Fann: Probably won't get much better than what I've already sent. I keep trying though

Baker: If you get me another like the one good one I will be so ecstatic

Fann: I'll see what I can do

Baker: 😍

Fann: I'll have her pick out her outfits later and sneak a pic

Baker: Nice

14. FANN and BAKER discussed plans to cause MV1 to unknowingly ingest substances that would render MV1 unconscious so that BAKER could have sexual contact with MV1. BAKER asked FANN to clarify whether she was serious about letting BAKER

have sexual access to MV1 while MV1 was unconscious. Consider the following exchange from on or about 7/26/2022:

Baker: Are you really going to let me play with [MV1]

Fann: As long as u can make sure we don't get caught

Baker: Well yea

Fann: Ok

Baker: Lol

Baker: So your ok with it

Fann: Just don't wake her up lol

Baker: That's the goal

Fann: Good cuz it won't end well if she does

Fann: She already threatens me with the cops cuz she's a little squirt

Baker: As long as you have an explanation why her parts may be sore

Baker: Which we can discuss

15. Around 8/03/2022, after FANN and BAKER were discussing Snapchat, FANN told BAKER "U took a screenshot." BAKER stated that he didn't mean to. FANN wanted him to delete the photo and BAKER claimed he did.

16. Other messages indicate that FANN was successful in her efforts to obtain sexually explicit photos of MV1 for BAKER. Consider the following exchange from on or about 8/5/2022:

Fann: Trying to make u happy [smiley emoji]

Baker: [smiley emoji]

Fann: That's the goal lol

Baker: Ik and you've done pretty well with the whole [MV1] thing

Fann: I try

Baker: Lol

Baker: Your def getting better

Baker: The one was so unexpected

Fann: Thought u might like it lol

Baker: Yessss very much can't wait for the next one

17. Other messages indicate that FANN was trying to accustom MV1 to the idea of sexual activity in preparation for sexual activity with BAKER. Consider this exchange from on or about 8/29/2022:

Fann: I'm trying to ease her into the whole sex thing but she still thinks everything is gross

Baker: Lol

Fann: I'm working on it lol

Baker: Snapchat

Fann: K

18. The effort to accustom MV1 to sexual activity included and apparent attempt to introduce MV1 to sex toys. In an exchange from on or about 8/31/20222, FANN told BAKER that she was going shopping, and she told BAKER she was "possible" going to get a "stuffie." BAKER responded, "Ahhhhhh/ A dildo for [MV1]?" FANN answered, "Not at the mall I'll do that in private."

19. There were several pictures saved within the Vault application on FANN's phone that depicted MV1 holding a dildo. One of them had a modification date of 8/31/2022, the same date in which BAKER asked whether FANN was going to purchase a dildo for MV1.

20. Several other pictures of MV1 were found in the Vault application on FANN's phone. One photo depicted MV1 completely nude. The photo appears to be focused on the nude body of the MV1 and her face is mostly out of frame of the photo. She is standing with her legs together and her genitals are not visible. She does not appear to be looking toward the camera. MV1 appears to be the same person depicted in the photo of the shirtless minor recovered from the search of the SnapChat account of Timothylb81.

21. BAKER is a registered sex offender. He was convicted in 2000 of criminal sexual conduct – second degree (person under 13). He is compliant with an active registration and his primary address is listed as 3115 Longstreet Ave SW, Wyoming MI. An alternate address is listed is 3102 Do-Mar Dr, Marne, MI.

22. On 7/15/2023, BAKER was arrested by the FBI and interviewed. BAKER

was read his Miranda Rights and agreed and answer questions on a question-by-question basis. BAKER confirmed that his main address was the trailer located at 3102 Do-Mar Dr in Marne. He was renting to own the property and he stayed there most nights. He claimed that he did not have many belongings at the 3115 Longstreet residence.

23. His girlfriend, AMANDA WARNER, who owned the 3115 Longstreet Ave residence, confirmed that he did not keep many items at her house. She claimed they only began dating again 3-weeks prior and that he stayed overnight there a couple of nights a week.

24. When BAKER was arrested and searched incident to arrest, a black Samsung cellular phone, IMEI 355802950227157, was taken off of his person.

CHARACTERISTICS COMMON TO INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

25. Based upon my knowledge, experience, and training in child exploitation and child pornography (CP) investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals with a sexual interest in children. These characteristics particularly apply to individuals involved in possessing or distributing CP online, including those accessing websites whose primary content is CP. These common characteristics include that the individuals:

a. Generally have a sexual interest in children and receive sexual gratification from viewing children engaged in sexual activity or in sexually suggestive poses,

or from literature describing such activity.

b. May collect or view sexually explicit or suggestive materials, in a variety of media, including in hard copy and/or digital formats. CP viewers and collectors oftentimes use these materials for their own sexual arousal and gratification. They may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse or groom a child to participate in sexual activity, or to demonstrate desired sexual acts to a child. They may also use toys, games, costumes, sexual clothing, sexual paraphernalia, and children's clothing to lure or entice children. They may keep "trophies" or mementos of sexual encounters with children, or items that they use to gratify a sexual interest in children, such as by collecting children's underwear or other items belonging to a child.

c. May take photographs that either constitute CP or indicate a sexual interest in children by using cameras, video cameras, web cameras, and cellular telephones. Such images and videos may be taken with or without the child's knowledge. This type of material may be used by the person to gratify a sexual interest in children.

d. Generally maintain their collections in a safe, secure, and private environment. These images and videos can be downloaded onto desktop or laptop computers, computer disks, disk drives, data disks, system disk operating systems, magnetic media floppy disks, Internet-capable devices, cellular telephones, tablets, digital music players, and a variety of electronic data storage

devices (hardware, software, diskettes, tapes, CDs, DVDs, SD cards, memory cards, USB/jump/flash memory devices, external hard drives, and other digital storage media). The images can be stored in both digital and hard copy format and are usually hidden so that they are not found by other members of the residence or by anyone else who enters the home. Such hiding places could include but are not limited to garages, sheds, attics, vehicles, bags, and pockets. Digital files and devices may be password protected, encrypted, or otherwise protected.

e. Often maintain their collections of CP and other materials indicating a sexual interest in children for a long period of time—commonly over the course of several years. These collections are also frequently maintained despite changes in residence or the acquisition of different or newer computer devices.

f. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from other CP distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, screen names, and telephone numbers of individuals with whom they have been in contact and who share the same interests in CP. Such correspondence may take place, for example, through online bulletin boards and forums, Internet-based chat messaging, email, text message, video streaming, letters, telephone, and in person. In some cases, these individuals may have joint involvement in CP activities with others within their household or

with whom they share a close relationship (e.g., brothers/siblings dating partners, or coworkers).

SPECIFICS OF SEIZING AND SEARCHING COMPUTER SYSTEMS

26. Computers and Internet-capable devices such as tablets and cellular telephones facilitate access to CP. The Internet affords collectors and viewers of CP several different venues for obtaining, viewing, and trading CP in a relatively secure and anonymous fashion.

27. Storage capacity of computers and portable storage media, such as USB or thumb drives, has grown tremendously within the last several years. These drives can store thousands of images at very high resolution, are easily transportable, and are relatively inexpensive. Advances in technology have significantly reduced the size of digital storage devices such that now large numbers of digital files can be stored on media that will fit in a person's pocket, on a keychain, or in any number of easily transportable and concealable places. An individual can now easily carry on his or her person storage media that contains thousands of files, including images, video files, and full-length movie files.

28. As with most digital technology, communications made from a computer device are often saved or stored on that device. Storing this information can be intentional, for example, by saving an email as a file on the computer or saving the location as a "favorite" website in a "bookmarked" file. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be

stored automatically in many places, such as temporary files or Internet Service Provider (ISP) client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files.

29. A forensic examiner often can recover evidence that shows whether a computer device contains peer-to-peer software, when the device was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten.

30. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the

ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

31. Searches and seizures of evidence from computers and computer devices commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search

of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

32. In order to retrieve data fully from a computer system, the analyst needs all storage devices as well as the central processing unit (CPU). In cases involving CP where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

33. To examine the computer and digital media properly, it may also be necessary to seize certain other items including documentation of programs, passwords, notes, or even specialized hardware. Therefore, this warrant seeks permission to seize not only the digital storage media and to search it for evidence in the form of CP images or videos, stored emails associated with the receipt and distribution of such images, and any chat or other text files relating to contact with collectors of CP or with actual children, but also requests permission to seize all hardware, software, and computer security devices necessary to access and examine the computer storage media. Peripheral

equipment including printers, routers, modems, network equipment used to connect to the Internet may also contain evidence of what devices were used to connect to the Internet, who used those devices, and what actions the person(s) performed while using such devices.

34. Forensic examiners can also find the presence or absence of certain software and programs to determine who controlled a computer at a given time. Such evidence includes: viruses, Trojan horses, spyware, malware, and other forms of malicious software; the presence or absence of security software designed to detect malicious software; the lack of malicious software; and the presence or absence of software designed to protect a device from infiltration, access, or control by another person or entity, which may include pop-up blockers, security software, password protection, and encryption. Forensic examiners can also find evidence of software or programs designed to hide or destroy evidence.

35. The time period required for a complete, safe, and secure forensic examination of the computer and storage media is uncertain. The government will make available for pick-up within a reasonable time all items found not to contain any contraband or material to be seized pursuant to the warrant and all hardware and software no longer needed for examination purposes. In conducting the search, the forensic examiner and agents will examine files regardless of their name because such names and file extensions can be altered to conceal their actual content. Because of the volume of data to be searched and the need to complete the examination in a reasonable

time, the forensic examiner will also use computer techniques such as keyword searches that may result in the display of irrelevant materials.

36. Attempts will be made to preview items on-scene, in order to exclude items unlikely to contain evidence or individuals with no involvement in the subject offenses. Items determined on-scene not to contain items listed in Attachment B will be left at the SUBJECT PREMISES. The remaining items will be seized and searched for further review or forensic examination and will be returned as soon as reasonably possible if they are determined not to contain evidence listed in Attachment B.

37. Retention of any computers would be warranted, if any CP is found thereon, in order to permit forfeiture of those computers and related properties as instrumentalities of the crime, pursuant to 18 U.S.C. §§ 2253(a)(3) and 2254(a)(2).

38. I am aware that the recovery of data by a computer forensic analyst takes significant time. For this reason, the Return inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the Return will not include evidence later examined by a forensic analyst.

CONCLUSION

39. Based upon the above information, I respectfully submit there is probable cause to believe that within the SUBJECT PREMISES and on the SUBJECT DEVICE there will be evidence of sexual exploitation and attempted sexual exploitation of children (18 U.S.C. § 2251(a)), distribution or receipt of child pornography (18 U.S.C.§ 2252A(a)(2)) and possession of child pornography (18 U.S.C. § 2252A(a)(5)(B)), the "subject offenses."

40. Wherefore, by this Continuation and Application, I respectfully request that the Court issue a Search Warrant authorizing the search of the SUBJECT PREMISES, described in Attachment A for items listed in Attachment B, and the seizure of those items for the purpose of searching and analyzing them off-site. I also respectfully request that the Court issue a Search Warrant authorizing the search of the SUBJECT DEVICE, described in Attachment A for items listed in Attachment B, and the seizure of those items for the purpose of searching and analyzing them off-site.

a. Because the search of the SUBJECT DEVICE will be performed using extraction software on a device that is already within FBI custody, the search of the SUBJECT DEVICE will not require further intrusion onto the real property of another. Moreover, extraction software must sometimes run for a continuous period of hours or days, making it impracticable to limit extraction efforts to just daytime hours. Accordingly, I submit there is a good cause to execute the search of the SUBJECT DEVICE at any time day or night.